WEB APPLICATION FIREWALL

FortiWeb-VM AWS Deployment Guide

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

December 12, 2017

FortiWeb-VM AWS Deployment Guide

1st Edition

Change log

12/12/2017	Initial release.

TABLE OF CONTENTS

Conventions

This document uses the conventions described in this section.

IP addresses

To avoid IP conflicts that would occur if you used examples in this document with public IP addresses that belong to a real organization, the IP addresses used in examples are fictional. They belong to private IP address ranges defined by these RFCs:

RFC 1918: Address Allocation for Private Internets

https://tools.ietf.org/html/rfc1918

RFC 5737: IPv4 Address Blocks Reserved for Documentation

https://tools.ietf.org/html/rfc5737

RFC 3849: IPv6 Address Prefix Reserved for Documentation

https://tools.ietf.org/html/rfc3849

Cautions, notes, & tips

This document uses the following guidance and styles for notes, tips and cautions:

	Warns you about procedures or feature behaviors that could have unexpected or undesirable results including loss of data or damage to equipment.
	Highlights important, possibly unexpected but non-destructive, details about a feature's behavior.
	Presents best practices, troubleshooting, performance tips, or alternative methods.

Typographic conventions

Convention	Example
Button, menu, text box, field, or check box label	From **Minimum log level**, select **Notification**.

CLI input	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI output	`FortiWeb# diagnose hardware logdisk info`
	`disk number: 1`
	`disk[0] size: 31.46GB`
	`raid level: no raid exists`
	`partition number: 1`
	`mount status: read-write`

Emphasis	HTTP connections are **not** secure and can be intercepted by a third party.
File content	<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>
Hyperlink	https://support.fortinet.com
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to **VPN > IPSEC > Auto Key (IKE)**.
Publication	For details, see the *FortiWeb Administration Guide*: https://docs.fortinet.com/fortiweb/admin-guides

Command syntax

The CLI requires that you use valid syntax, and conform to expected input constraints. It will reject invalid commands.

For command syntax conventions such as braces, brackets, and command constraints, see the *FortiWeb CLI Reference*:

http://docs.fortinet.com/fortiweb/reference

Introduction

This deployment guide provides instructions to configure FortiWeb-VM on Amazon Web Services (AWS), including the Amazon Virtual Private Cloud (VPC) and Amazon Elastic Compute Cloud (EC2), to protect your AWS web-based application environment.

FortiWeb-VM instances running on AWS provide the same functionality as FortiWeb hardware-based platforms with the added flexibility to deploy instances as needed to meet the demands of your AWS web-based application environment.

To configure and deploy FortiWeb-VM on AWS, follow these steps:

1. Create an Amazon VPC. For details, see "Creating an Amazon VPC" on page 9.
2. Optionally, configure a custom Security Group for a FortiWeb-VM instance. For details, see "Creating a Security Group" on page 11.
3. Launch a FortiWeb-VM instance via the Amazon EC2 Dashboard. For details, see "Deploying FortiWeb-VM on the Amazon VPC" on page 14.
4. Connect to a FortiWeb-VM instance. For details, see "Connecting to the FortiWeb-VM Instance" on page 16.

Amazon VPC

Amazon VPC allows you to provision a logically isolated section of AWS from which you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selecting your own IP address range, creating subnets, and configuring route tables and network gateways. You can also create a Hardware Virtual Private Network (VPN) connection between your datacenter and the VPC to leverage the AWS cloud as an extension of your datacenter.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that have access to the Internet and place your backend systems, such as databases and application servers, in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to instances in each subnet.

For more information, see the *Amazon VPC Documentation*:

https://aws.amazon.com/documentation/vpc

Amazon EC2

Amazon EC2 allows you to scale the Amazon VPC by renting virtual computers on which to run FortiWeb-VM instances. You can create, launch, and end FortiWeb-VM instances running on the Amazon VPC according to your environment's needs. You'll deploy and run FortiWeb-VM instances using Amazon Machine Images (AMIs) hosted on the Amazon Marketplace; licensed and BYOL FortiWeb-VM instance types are available.

For more information, see the *Amazon EC2 Documentation*:

https://aws.amazon.com/documentation/ec2

Scope

This document describes the steps required to:

- Create an Amazon VPC.
- Configure a custom Security Group for a FortiWeb-VM instance.
- Launch a FortiWeb-VM instance via the Amazon EC2 Dashboard.
- Connect to a FortiWeb-VM instance.

This document does **not** describe the steps required to configure FortiWeb to monitor and protect your AWS web-based application environment. For those instructions, see the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

Requirements

To deploy FortiWeb-VM on AWS, you must:

- Have an AWS account. If you don't already have an AWS account, register at https://aws.amazon.com; please note that you'll have to provide billing information.
- If you'll be deploying BYOL instance types, have a valid license for each FortiWeb-VM that you plan to deploy. If you don't have a valid license for each FortiWeb-VM instance that you plan to deploy, contact your reseller.

Creating an Amazon VPC

This section provides instructions to create a VPC for FortiWeb-VM with the Amazon VPC wizard. The Amazon VPC wizard will create a VPC with an IPv4 CIDR block, attach an Internet gateway to the VPC, create an IPv4 subnet in the VPC, and create a custom route table associated with the subnet.

Once you create the VPC according to the below instructions, create a Security Group. For details, see "Creating a Security Group" on page 11.

If you do not have an AWS account, register for one now. To do so, go to https://aws.amazon.com; please note that you'll have to provide billing information.

You cannot continue without an AWS account.

For more information about creating a VPC, see "Step 1: Create the VPC" in the *Amazon VPC Documentation*:

http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-ipv4.html#getting-started-create-vpc

To create an Amazon VPC

1. Go to the Amazon VPC console at https://console.aws.amazon.com/vpc.

Confirm that the current region is the region in which you intend to create the VPC. To do so, observe the current region in the top-right of the navigation bar. If you want to create the VPC in a different region, you must change the region now.

Once the VPC is created, you will **not** be able to launch an instance from a different region.

2. From the navigation bar, click **Services**.
3. Under **Networking & Content Delivery**, select **VPC**.
4. Under **Resources**, click **Start VPC Wizard**.
5. Choose **VPC with a Single Public Subnet**.
6. Click **Select**.
7. Verify or modify these settings:

IPv4 CIDR block	Displays the default IPv4 address range for the VPC. If you want to specify a different CIDR block, delete the default CIDR block and enter a new one here. The allowed block size is between a `/16` netmask and `/28` netmask. For details, see "VPC and Subnet Sizing" in the *Amazon VPC Documentation*:

	http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing.
IPv6 CIDR block	Select **No IPv6 CIDR Block**.
VPC name	Enter a name for the VPC. You will use the name to reference the VPC in other parts of the configuration.
Public subnet's IPv4 CIDR	Displays the default IPv4 address range for the public subnet. If you want to specify a different CIDR block for the subnet, delete the default CIDR block and enter a new one here. The allowed block size is between a `/16` netmask and `/28` netmask. For details, see "VPC and Subnet Sizing" in the *Amazon VPC Documentation*: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Subnets.html#VPC_Sizing.
Availability Zone	Displays the Availability Zone for the public subnet. Select between: • **No preference** so that the VPC will select the optimal Availability Zone for the VPC. • A specific Availability Zone. For details, see "Regions and Availability Zones" in the *Amazon VPC Documentation*: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html
Subnet name	Enter a name for the public subnet of the VPC. You will use the name to reference the public subnet in other parts of the configuration.
Service endpoints	Optionally, click **Add Endpoint** to configure a connection directly to an AWS service without a gateway, NAT device, VPN connection, or AWS Direct Connect connection. You can add endpoints to multiple AWS services. Because traffic between the VPC and AWS services does not leave the AWS network when you use endpoints, endpoints allow the VPC to communicate with AWS services without imposing resource costs on your network. If you click **Add Endpoint**, you must also configure the **Service**, **Subnet**, and **Policy** for the endpoint. You do **not** have to add endpoints when hosting FortiWeb-VM on AWS to protect your web-based application environment. For more information about adding an endpoint, see "VPC Endpoints" in the *Amazon VPC Documentation*: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-endpoints.html
Enable DNS	This guide provides instructions to connect to the FortiWeb-VM

hostnames	instance assuming that this setting is enabled. Optionally, select **Yes** so that instances that are launched into the VPC receive a DNS hostname. For details, see "Using DNS with Your VPC" in the *Amazon VPC Documentation*: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-dns.html Enable this setting so that you can easily connect to the instance using the public DNS address.
Hardware tenancy	Configure this option to select whether instances launched in the VPC run on shared or dedicated hardware. Select one of the following options: • **Default**—The instance runs on shared hardware. • **Dedicated**—The instances runs on single-tenant hardware. • **Host**—The instance runs on a dedicated host, which is an isolated server with configurations that you can control. **Note**: Selecting **Dedicated** or **Host** incurs additional costs. For details, see "Dedicated Instances" in the *Amazon VPC Documentation*: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/dedicated-instance.html
Enable ClassicLink	Optionally, if your account supports Amazon EC2-Classic, select **Yes** so that you can link an EC2-Classic instance to the VPC. For details, see "ClassicLink" in the *Amazon EC2 Documentation*: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/vpc-classiclink.html

8. Click **Create VPC**.

   The Amazon VPC Wizard may take a few minutes to create the VPC.

9. From the **VPC Dashboard** menu on the left, go to **Virtual Private Cloud > Your VPCs**. Take note of the **Name** and **VPC ID** of the VPC that you just created; you will need this information to identify components of the VPC later and log in to the instance.

Creating a Security Group

This section provides instructions to create a Security Group for a FortiWeb-VM instance in the VPC. By default, when you create a VPC, a default Security Group protects instances in it. If you don't specify a Security Group when launching an instance in the VPC, the default Security Group will protect that instance.

Because FortiWeb-VM will be monitoring and protecting the VPC, you need to specify a custom Security Group for the FortiWeb-VM instance. There are two options to specify a custom Security Group:

1. Select a predefined Security Group when launching a FortiWeb-VM instance. This Security Group is generated by Fortinet. If needed, you can include additional rules according to your environment's needs when specifying this predefined Security Group. For details, see Step 19 on page 15 in "Deploying FortiWeb-

VM on the Amazon VPC".

2. Create a custom Security Group. If you create a custom Security Group, you will need to include rules that allow FortiWeb-VM to connect and run properly. For details, see "To create a Security Group for FortiWeb-VM" on page 12.

For more information about creating a Security Group, see "Step 2: Create a Security Group" in the *Amazon VPC Documentation*:

http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-ipv4.html

To create a Security Group for FortiWeb-VM

1. Go to the Amazon VPC console at https://console.aws.amazon.com/vpc.
2. From the navigation bar, click **Services**.
3. Under **Networking & Content Delivery**, select **VPC**.
4. From the **VPC Dashboard** menu on the left, go to **Security > Security Groups**.
5. Click **Create Security Group**.
6. Configure these settings:

Name tag	Optionally, enter a key-value pair to tag the Security Group so that you can reference it in the VPC. For details, see "Tagging Your Amazon EC2 Resources" in the *Amazon EC2 Documentation*: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html
Group name	Enter a name for the Security Group.
Description	Enter a description for the Security Group. This description will be viewable from the list of Security Groups in the VPC Dashboard.
VPC	Optionally, select a VPC to which you want to apply the Security Group. You can also specify a Security Group when launching an instance in a VPC.

7. Click **Yes, Create**.
8. From the list of Security Groups, select the one you just created.
9. Below the list of Security Groups, select the **Inbound Rules** tab.
10. Click **Edit**.
11. Click **Add another rule** for as many rules as you need to create.

12. Configure the following rules so that FortiWeb will connect and run properly:

Rule #1

Type	SSH
Protocol	TCP
Port Range	22
Source	**Custom**—0.0.0.0/0
Description	Optionally, enter a description for the rule.

Rule #2

Type	HTTP
Protocol	TCP
Port Range	80
Source	**Custom**—0.0.0.0/0
Description	Optionally, enter a description for the rule.

Rule #3

Type	HTTPS
Protocol	TCP
Port Range	443
Source	**Custom**—0.0.0.0/0
Description	Optionally, enter a description for the rule.

13. Configure additional rules according to your environment's needs.
14. Click **Save**.

Deploying FortiWeb-VM on the Amazon VPC

This section provides instructions to deploy a FortiWeb-VM EC2 instance in the VPC. The Amazon EC2 launch wizard will help you deploy FortiWeb-VM using an Amazon Machine Image (AMI) from the AWS Marketplace.

For more information about deploying an instance on the VPC, see "Step 3: Launch an Instance into Your VPC" in the *Amazon VPC Documentation*:

http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-ipv4.html#getting-started-launch-instance

To deploy a FortiWeb-VM EC2 instance on the Amazon VPC

1. Go to the Amazon VPC console at https://console.aws.amazon.com/vpc.

Confirm that the current region is the region in which you created the VPC. To do so, observe the current region in the top-right of the navigation bar. If the current region is a different region than the region in which the VPC was created, you must change the region now.

2. From the navigation bar, click **Services**.
3. Under **Networking & Content Delivery**, select **VPC**.
4. Under **Resources**, click **Launch EC2 Instances**.
5. From the navigation menu on the left, select **AWS Marketplace**.
6. In the search bar, enter `FortiWeb`.
7. **Select** the FortiWeb-VM AMI that you want to deploy. Choose one of the following:
   - **Fortinet FortiWeb-VM Web Application Firewall**—usage-based AMI.
   - **Fortinet FortiWeb-VM Web Application Firewall (BYOL)**—BYOL AMI. If you're deploying a BYOL AMI, you must have a FortiWeb-VM license for each FortiWeb-VM that you deploy on the VPC.

Pricing options based on Instance Type are available when you select an AMI.

8. Click **Continue**.
9. Select the **Instance Type** according to your environment's needs. If you're deploying a BYOL AMI, select an **Instance Type** that's compatible with your FortiWeb-VM license. For example, if your FortiWeb-VM license supports up to 8 vCPUs, select an **Instance Type** that supports up to 8 vCPUs.

   For details, see "Amazon EC2 Instance Types" in the *Amazon EC2 Documentation*:

   https://aws.amazon.com/ec2/instance-types
10. Click **Next: Configure Instance Details**.
11. For **Network**, select the VPC that you created in "Creating an Amazon VPC" on page 9.

12. For **Subnet**, select the public subnet that you created in "Creating an Amazon VPC" on page 9.
13. Leave the other options at their default settings for now. Click **Next: Add Storage**.
14. For the `Root` **Volume Type**, change the **Size** to `30`.
15. Click **Next: Add Tags**.
16. Click **Add Tag**.
17. Include a Key-Value pair for the FortiWeb-VM instance so that you can reference it in the VPC.

    For **Key**, enter `Name`.

    For **Value**, enter a descriptor such as `FortiWeb-VM1`.

You can use tags to define values to help reference instances, elements of instances (e.g., private and public IP addresses), and other Amazon EC2 resources in the VPC. For details, see "Tagging Your Amazon EC2 Resources" in the *Amazon EC2 Documentation*:

http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Using_Tags.html

18. Click **Next: Configure Security Group**.

    By default, Amazon places the VPC behind a basic firewall. Because you're deploying FortiWeb-VM, you need to remove Amazon's default protection.

19. For **Assign a security group**, choose one of the following:

    - **Create a new security group**—Select to implement a Security Group called **Fortinet FortiWeb-VM Web Application Firewall-v5-8-2-AutogenByAWSMP-10** that consists of default rules for FortiWeb-VM. If you need to add more rules according to your environment's specific needs, click **Add Rule** to configure those rules.
    - **Select an existing security group**—Select to implement a custom Security Group that you already created in "Creating a Security Group" on page 11.

20. Click **Review and Launch**.

    Verify the details of the FortiWeb-VM instance.

21. Click **Launch**.

    A dialog box appears titled **Select an existing key pair or create a new key pair**.

22. From the drop down menu, choose **Proceed without a key pair**.
23. Click the acknowledgment check box.
24. Click **Launch Instances**.

Connecting to the FortiWeb-VM Instance

This section provides instructions to connect to the FortiWeb-VM instance. You can connect via two methods:

- Use an SSH connection to connect via the CLI. For details, see "Connecting via the CLI" on page 16.
- Use a web browser to connect via the web UI. For details, see "Connecting via the web UI" on page 17.

To connect to the FortiWeb-VM instance, connect via the public DNS address and log in to the `admin` account using the VPC ID of the FortiWeb-VM instance for the password. For details, see "To locate the public DNS address and VPC ID of the FortiWeb-VM instance" on page 16.

If three incorrect login attempts occur in a row, FortiWeb temporarily blacklists your IP address to protect against brute force login attacks. After one minute, you can attempt to log in again.

Once you connect to the FortiWeb-VM instance, complete these tasks:

1. Change the default password. For details, see "Changing the default admin password" on page 17.
2. Modify the default web administration ports. For details, see "Modifying the default web administration ports" on page 18.

Once you connect to the FortiWeb-VM instance, change the default password. For details, see "Changing the default admin password" on page 17.

To locate the public DNS address and VPC ID of the FortiWeb-VM instance

1. Go to the Amazon VPC console at https://console.aws.amazon.com/vpc.
2. From the navigation bar, click **Services**.
3. Under **Networking & Content Delivery**, select **VPC**.
4. From the **VPC Dashboard** menu on the left, go to **Virtual Private Cloud > Your VPCs**.
5. Take note of the **Public DNS address** and **VPC ID** of the instance for the password.

Connecting via the CLI

You must use terminal emulation software to connect to the FortiWeb-VM instance via the CLI. This example shows you how to connect via the CLI using PuTTY (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html). If you use another terminal emulation software, the steps may be different.

Note: Regardless of the terminal emulation software that you use, remove any environment variables before attempting to connect to the FortiWeb-VM instance.

To connect via the CLI

1. Start PuTTY.
2. In the **Category** tree, expand **Connection**.

3. Click **Data**.
4. Remove any environment variables.
5. In the **Category** tree, click **Session**.
6. For **Host Name (or IP address)**, enter the public DNS address of the FortiWeb-VM instance.
7. For **Port**, enter `22`.
8. For **Connection type**, select **SSH**.
9. Click **Open**.
10. Click **Yes** to verify the fingerprint and accept the FortiWeb-VM's SSH key.
11. Enter `admin` for the username and press Enter.
12. Enter the VPC ID for the password and press Enter.

    Note: If the VPC ID is longer than 32 characters, the password is only the first 32 characters of the VPC ID.
13. Upon successfully logging in, you will see this prompt:

```
fortiweb #
```

Connecting via the web UI

You must use a web browser with Adobe Flash Player 10 or later to connect via the web UI.

To connect via the web UI

1. Open a compatible web browser.
2. Enter the public DNS address of the FortiWeb-VM instance.
3. For **Name**, enter `admin`.
4. For **Password**, enter the VPC ID

   Note: If the VPC ID is longer than 32 characters, the password is only the first 32 characters of the VPC ID.
5. Upon successfully logging in, you will see the dashboard of the web UI.

Changing the default `admin` password

When you first log in to the FortiWeb-VM instance, you should change the password for the `admin` account. You can change the default password either via the CLI or the web UI—below are instructions for both options.

To change the `admin` password in the CLI

Enter the following commands:

```
config system admin
   edit admin
      set password <password_str>
```

```
        next
    end
exit
```

where <password_str> is the new password for the admin account. Once you enter set password <password_str>, you will be prompted to confirm the password.

To change the admin password in the web UI

1. Log in to the admin account.
2. Go to **System > Admin > Administrators**.
3. Select the **admin** account.
4. Click **Change Password**.
5. Configure these settings:

Old Password	Enter the current password. **Note**: If this is your first time changing the password, the password will be the VPC ID.
New Password	Enter a new password. The maximum length is 32 characters. **Note**: If you enter a password that contains more than 32 characters, the first 32 characters will become the password.
Confirm Password	Enter the new password again.

6. Click **OK**.

   You will be logged out of the web UI. Enter the username and new password to log in again.

Modifying the default web administration ports

This section provides instructions to specify the TCP port number on which FortiWeb-VM listens for HTTP and HTTPS administrative access. Because FortiWeb-VM is running on AWS, you need to specify custom port numbers for incoming connections destined for FortiWeb-VM itself.

This task can be completed either in the CLI or the web UI. See below for instructions.

To modify the default web administration ports in the CLI

Enter the following commands:

```
config system global
   set admin-port <port_int>
   set admin-sport <port_int>
end
```

Variable	Description	Default
`admin-port <port_int>`	Enter the port number on which FortiWeb-VM listens for HTTP access to the web UI. The valid range is 1–65,535.	`80`
`admin-sport <port_int>`	Enter the port number on which FortiWeb-VM listens for HTTPS (SSL-secured) access to the web UI. The valid range is 1–65,535.	`443`

To modify the default web administration ports in the web UI

1. Log in to the web UI.
2. Go to **System > Admin > Settings**.
3. Configure these settings:

HTTP	Enter the port number on which FortiWeb-VM listens for HTTP access to the web UI. The valid range is 1–65,535.
HTTPS	Enter the port number on which FortiWeb-VM listens for HTTPS (SSL-secured) access to the web UI. The valid range is 1–65,535.

4. Click **Apply**.